



UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/743,653	03/14/2001	Ahmet Mursit Eskicioglu	RCA 89131	7330

7590 11/15/2005  
Joseph S Tripolis  
Thomson Multimedia Licensing Inc  
PO Box 5312  
Princeton, NJ 08540

EXAMINER

DAVIS, ZACHARY A

ART UNIT PAPER NUMBER

2137

DATE MAILED: 11/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



### DETAILED ACTION

1. A Request for Continued Examination with amendment was received on 29 August 2005. Claims 1, 4, 6, and 7 have been amended. Claim 5 has been canceled. New Claims 8-17 have been added. Claims 1-4 and 6-17 are currently pending in the present application.

#### ***Response to Arguments***

2. Applicant's arguments with respect to claims 1-4, 6, and 7 have been considered but are moot in view of the new ground(s) of rejection.

#### ***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-4, 7-10, and 12-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kudelski et al, US Patent 5144663, in view of Schneier, *Applied Cryptography*.

Art Unit: 2137

In reference to Claims 1 and 7, Kudelski discloses a method for managing access to a restricted transmitted event including receiving and decrypting encrypted access information (column 6, lines 4-10) which includes data corresponding to the price of the transmitted event (column 3, lines 6-13 and 42-50), verifying that the cost of the event is less than a pre-stored cash reserve (column 6, lines 35-41), and receiving and descrambling the scrambled transmitted event (column 4, lines 5-19). Kudelski further discloses that the encrypted access information may be encrypted using any encryption system (column 4, lines 54-57); however, Kudelski does not explicitly disclose using a public key system for encrypting the access information.

Schneier discloses hybrid cryptosystems in which a symmetric key is distributed securely by encrypting the symmetric key with a public key at the sender and decrypting the symmetric key with the private key at the receiver (page 33). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Kudelski by encrypting the access information using a public key, in order to gain the benefits of a hybrid cryptosystem, namely the speed of symmetric encryption with less risk of the key being exposed (see Schneier, page 33). However, the cited portions of Schneier are silent as to whether a public key would be shared between a plurality of service providers, as in Claim 1, or if each service provider would have its own public key, as in Claim 7.

Specifically in reference to Claim 1, official notice is taken that it is well known that a smart card as used by Kudelski for storing a key (column 4, lines 58-63) generally has limited storage space, and therefore that it would have been obvious to one of

Art Unit: 2137

ordinary skill in the art at the time the invention was made to have a plurality of service providers share a public key, in order to conserve storage space by only requiring the smart card to store one private key corresponding to the one public key.

Specifically in reference to Claim 7, official notice is taken that it would have been obvious to one of ordinary skill in the art at the time the invention was made to assign a different respective public key/private key pair to each service provider, in order to minimize the damage done if one private key was compromised. Further, it would have been obvious to select from a plurality of private keys the private key associated with the public key of the particular service provider that was used for encryption and use that selected private key for the decryption.

In reference to Claims 2 and 8, Kudelski further discloses that the access information includes a descrambling key (column 6, lines 6-10) and purchase information including channel identification data, event identity data, date and time stamp data, and billing data (column 6, lines 11-50).

In reference to Claims 3 and 9, Kudelski further discloses transferring data associated with the purchased event to update a user's account information (column 8, lines 48-58).

In reference to Claims 4 and 10, Kudelski further discloses a smart card (column 4, lines 58-63).

In reference to Claims 15 and 12, Kudelski further discloses that the transmitted event can be audio/video program data (see column 1, lines 17-22; column 3, lines 6-20).

In reference to Claims 16 and 13, Kudelski further discloses that a service provider can be a television or cable network (see column 1, lines 13-23; column 3, lines 46-50).

In reference to Claims 17 and 14, Kudelski further discloses that the transmitted event can be a package of programs (column 7, line 65-column 8, line 5, where a subscription can be purchased).

5. Claims 6 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kudelski in view of Schneier as applied to claims 4 and 10 above, and further in view of EBU Project Group, "Functional Model of a Conditional Access System".

Kudelski as modified by Schneier discloses everything as applied to Claim 5; however, Kudelski as modified above does not explicitly disclose the use of the PCMCIA card standard in the smart card. EBU discloses that a smart card used in a conditional access system may use the PCMCIA standard (page 69, section 3.4). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Kudelski as modified by Schneier to use the PCMCIA standard for the smart card, in order to allow the system to contain the conditional access system and the descrambler in a single unit (see EBU, page 69, section 3.4).

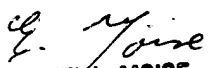
**Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

zad

  
EMMANUEL L. MOISE  
SUPERVISORY PATENT EXAMINER